JOHN FARINA

john.farina95@gmail.com ❖ (404) 655-8823 ❖ github.com/JFarina5 ❖ jfarina5.github.io ❖ linkedin.com/in/jfarina5

WORK EXPERIENCE

Fortra

Cybersecurity Researcher II | Oct. 2021 – Present

- Automated monthly reporting using Python, Matplotlib, NumPy, PostgreSQL integration (Psycopg2), and dynamic report templates, reducing processing time from weeks to seconds
- Implemented advanced Artificial Intelligence (AI) technologies, including Large Language Models (LLMs), on internal and AWS EC2 servers to generate insightful reports from historical PostgreSQL data
- Integrated LLMs/AI into the internal tool-set for proactive threat actor communication analysis
- Developed an advanced external honeypot with Flask and JavaScript to accurately log threat actor metadata
- Engineered a specialized Python module utilizing Pandas and Matplotlib, streamlining charting processes within the research team and facilitating smoother data visualization across the organization
- Led the development of robust Python APIs using Flask, enabling complex queries for efficient bulk extraction of critical company data, significantly improving operational efficiency
- Conducted comprehensive analysis on customer-submitted suspicious links and files
- Proactively reviewed and validated rules governing customer emails, using internal applications to assess threat levels
- Administered Amazon Web Services (AWS) infrastructure, deploying EC2 instances and reinforcing security policies
- Conducted covert operations within forums, chatrooms, and websites to gather intelligence on threat actor operations

National Security Agency

Computer Network Defense Analyst / Team Lead | June 2019 – Oct. 2021

- Assessed network and end-point behavior that threaten customer networks to detect and mitigate cyberspace threats
- Utilize C++ to aid in developing signatures used to sort through network traffic and identify malicious cyber activity
- Utilized Python and Jupyter notebooks to develop solutions for analytical problems
- Executed triage processes by efficiently tracking targets, observing abnormalities in network traffic, and reporting valuable intelligence, all in an attempt to assess and prioritize leads against the given target-set
- Produced reporting on adversary tools, techniques, and procedures (TTPs) to be viewed Agency-wide
- Served in an active Team Lead position managing twenty-four civilian, military, and contractor personnel

National Security Agency

Target Digital Network Analyst | May 2018 – Aug. 2018

- Applied computer-based programs alongside Python and C++ to process data for analytical problems
- Conducted Trend analysis against network/cyber activity to determine target traffic behavior patterns
- Conducted target analysis, target research, and analysis of metadata
- Selected, built, and developed query strategies against appropriate collection databases

EDUCATION

B.S. Computer Science, Concentration in Information Security – *University of North Georgia, May 2019*
A.S. Computer Science – *University of North Georgia, May 2017*
Security+ – *CompTIA, March 2020*

SKILLS

Programming Languages: Python, Java, Dart, C++, C, C#, Ruby, SQL, Dart, Swift, XML, HTML, CSS, PowerShell, Bash
Frameworks: Matplotlib, Pandas, Numpy, Seaborn, Flask, Geopandas, smtplib, Ruby on Rails, PyTorch, FastAPI, Psycopg2
Developer Tools: GitHub, GitLab, Git, Docker, AWS, Jenkins, Confluence
Security Tools: Wireshark, Nmap, Metasploit, Nessus, Burp Suite, Censys, Shodan, Cobalt Strike, Tenable